

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

EPIC GAMES, INC.,

Plaintiff,

v.

APPLE INC.,

Defendant.

CASE NO. 4:20-CV-05640-YGR

**DECLARATION OF MARK G. GRAFF**

1 I, Mark G. Graff, declare as follows:

2 1. I am a consulting cybersecurity practitioner and author. I submit this declaration in  
3 support of Apple's position with respect to Epic's request for an injunction.

4 2. My opinion in this matter is based on my experience as a defender against cyberattacks,  
5 as a computer programmer of several decades' standing, and as a technical manager. As the head of  
6 cybersecurity for Lawrence Livermore National Laboratory, and later as the Chief Information Security  
7 Officer (CISO) of NASDAQ, I was responsible for anticipating cyber threats and defending those  
8 institutions against spies and world-class cyber criminals. In 2003, I co-wrote the earliest book ("Secure  
9 Coding") describing how to develop, test, and deploy software so as to make it resistant to attack, and  
10 have since co-written two others on the subject of security and software. I have also managed teams of  
11 software developers and specialists responsible for analyzing and improving the security of application  
12 software. As an expert witness, I have twice testified before Congress on matters of Internet and  
13 software security; supported the Federal Trade Commission in a lawsuit relating to software security  
14 and consumer safety; and helped California litigate a case regarding election security. In other work as  
15 a consultant, I have written software to help control nuclear reactors as well as alarm systems for  
16 museums and banks. More information about my work experience can be found in the curriculum vitae  
17 I have attached as Exhibit A.

18 3. My comments in this declaration are based on my reading of Epic's Complaint; several  
19 declarations in support and opposition (including particularly those of Mr. Grant and Mr. Schiller); and  
20 other public documents in this case. I also asked for and received from Apple certain statistics regarding  
21 App Store operations (see paragraph 6), and a copy of the description Epic supplied (see paragraph 14)  
22 when submitting its Fortnite update to the App Store on August 3, 2020; other than these two sets of  
23 facts, I have not made use of any non-public information about Apple's operations.

24 4. My general conclusion is that, based on cybersecurity considerations, Apple acted  
25 reasonably on August 14, 2020 when it suspended Epic's membership in the Apple Developer Program.  
26 This conclusion is explained in the following paragraphs. I think also, as I will explain in this  
27 declaration, that Apple's published App Store review policies and procedures are well considered; that  
28 Epic's failure to disclose its new non-IAP payment feature, when submitting its v13.40 Fortnite update

1 on August 3, obstructed informed review by Apple; and that if the way Epic performed the update  
2 becomes the norm for other developers, the effectiveness of Apple's security reviews of submitted apps  
3 will be impeded, resulting in increased risk for Apple's customers and others, worldwide.

4 5. Apple's role as the steward of security and privacy in applications submitted to the App  
5 Store is a substantial responsibility, in light of the risks to customers and others should a rogue  
6 application pass review and be deployed. Application software must be closely scrutinized, both when  
7 originally submitted and when any changes are made that either introduce new features; make use of  
8 new resources such as files or user input; or alter program logic or operational flow. Careful analysis  
9 and custom functionality-based testing affords the best barrier to malefactors – whether individual  
10 criminals, organized crime elements, or nation-state intelligence services – lodging malware into  
11 pockets and purses around the world.

12 6. In order to gauge the reasonableness of Apple's App Review policies and procedures, I  
13 believe it is helpful to consider the sheer volume of the task, including the number of developers or  
14 companies that attempt changes inconsistent with Apple's App Store review policies pertinent to this  
15 case. Accordingly, while preparing this declaration I asked for and received the following statistics.  
16 Apple tells me that so far this calendar year, they have processed 4,013,571 apps. In the last twelve  
17 months alone, they have terminated 48,297 developer accounts for what they call "Bait & Switch /  
18 Illicit Concept Changes"; terminated 54,805 accounts for "Hidden features / Code Obfuscation /  
19 Facilitating downloading/installing of executable code, etc."; and terminated 1,197 accounts for  
20 "introducing a non-IAP payment method". (I discuss in paragraph 18 how Epic's actions may relate to  
21 these categories.)

22 7. These numbers say to me that, first, Apple's review process must necessarily include  
23 significant automation. Yet my experience with application review has shown over and over the value  
24 of proceduralized but flexible human analysis, and so I was glad to learn from the material Apple  
25 provided that "[a]ll apps are installed on actual devices and *reviewed by a person* [emphasis added]."  
26 This mix of automated and human review is the best approach for identifying security risks with  
27 candidate apps. But the effectiveness of this testing will be hindered – and the risk of security violation  
28

1 or misadventure increased – if either the software itself or the submitting developer obfuscates what  
2 the app does and the way it works.

3 8. Application security is the discipline of designing, developing, testing and deploying  
4 software so as to be resistant to attack, preserving the integrity of the program’s actions under adverse  
5 conditions. “Threat modeling” is the practice of imagining potential cyberattacks, then reasoning about  
6 the attributes of a system that would either prevent, allow, or even facilitate such an attack; and also,  
7 how the systems can be hardened, and the consequences abated. Application review processes, an  
8 important part of application security, typically use specialized testing software to examine whether  
9 the software under test could be manipulated to produce the loss scenarios envisioned in the security  
10 threat models. The automated tests can examine the precise instructions and data structures within the  
11 software, searching for and calling out either security weaknesses (“vulnerabilities”) that may make  
12 the application exploitable by bad actors, or explicitly intended bad behavior such as theft or disclosure  
13 of private information. Ideally, the combination of automated testing and human review will not only  
14 detect sheer poor programming practice (e.g., not allocating sufficient storage for input data) but also  
15 gauge the relevance of the candidate app to previously developed threat models. (An application  
16 dealing with payment, for example, might be checked to make sure amounts are handled accurately,  
17 and that identity and account information is protected from potential prying eyes.) But tests and human  
18 analysis are not infallible and can fail to find serious problems – especially if the body of software to  
19 be reviewed is lengthy and complex, and even more so without the cooperation of developers in  
20 pointing out key changes and functionality.

21 9. The scale of what is at stake with the Apple App Store review process is remarkable.  
22 While I have not seen any threat models Apple may use in devising its review processes, it is easy to  
23 see that a rogue application affecting the operation of a significant fraction of the world’s iPhones could  
24 substantially disrupt local or even worldwide telephony systems, as well as broad segments of the  
25 Internet itself. These risks mean that Apple, as steward of software running on about a billion devices  
26 worldwide, needs policies and practices that protect against such potential attacks while not needlessly  
27 impeding the flow of application software to its customers’ phones. In my opinion, Apple’s App Store  
28 Review Guidelines (see Declaration of Philip W. Schiller in opposition to a TRO, Exhibit C) are

1 reasonable; it is appropriate and responsible to institute requirements allowing Apple to carry out an  
2 informed, substantive, functionality-specific review of app functionality and operation.

3 10. I turn now to my comments concerning the declaration of Mr. Andrew Grant in support  
4 of Epic's motion.

5 11. Let me point out first that one of the biggest challenges in cyberdefense is the  
6 "executable content" problem. (Here I am using "executable content" as an umbrella term to describe  
7 code that a computer may be directed to execute that has been either created from inside the program,  
8 during its execution or dynamically transferred to the computer in the course of its executing other  
9 code. One simple example of executable content is the JavaScript text that your browser can encounter  
10 when you visit a particular website.) Classic "static" code is written, compiled, and then executed.  
11 There are many tools available today to examine static code to check for security holes; and software  
12 producers often build the use of these tools into the software development process, making the software  
13 safer and more difficult to exploit. When code is downloaded dynamically and executed on the fly, it  
14 is more difficult to check for security holes – and often, thorough checking is impractical, since a user  
15 (or an urgent task) may be waiting for the code to run.

16 12. Now the Fortnite change central to this dispute does not apparently make use, precisely,  
17 of executable content, as Mr. Grant points out (e.g., in paragraph 13 of his declaration in support of a  
18 TRO). Instead, the change involved a "hotfix" (described in paragraph 4 et seq.). As Mr. Grant explains  
19 (in paragraph 10 of his declaration), "When *Fortnite* is opened on an iOS device, the application  
20 connects to Epic's servers to check for new content to download or for 'notice' to make pre-existing  
21 functionality or content accessible." He continues (paragraph 13), "[On] August 13, 2020, when the  
22 *Fortnite* app on iOS devices queried Epic's servers as to how many payment processing options were  
23 available, the servers informed the app that there were two options... [and] the code made both options  
24 accessible to users." Mr. Grant concludes his hotfix discussion with the statement, "*Epic did not*  
25 *download any executable code or interpreted code in the Fortnite app as part of the hotfix that made*  
26 *the payment options available* [emphasis added]."

27 13. In my opinion, Mr. Grant's statement that Epic "did not download any executable code  
28 or interpreted code" makes a distinction without a difference. Mr. Grant states in paragraph 12 of his

1 TRO declaration that “On August 3, 2020, Epic submitted Version 13.40 of *Fortnite* for review by  
2 Apple... [that] included a payment process interface.” That new payment interface was then rendered  
3 operational by a change on Epic’s servers on August 13, as detailed in paragraph 13. That is, new code  
4 was submitted on August 3 that contained a latent feature activated 10 days later. To me, the fact that  
5 the new functionality was delivered in two parts instead of one is not a significant difference. From a  
6 security point of view, what matters most is whether Epic’s actions meant that the change was not  
7 properly subject to review by Apple. With regard to Apple’s statement (Schiller TRO declaration,  
8 Exhibit I, paragraph 4) that the app “[downloaded] new code,” I point out that new code was in fact  
9 put in place on August 3, *via the updating submittal*. Again, the pivotal security point is whether the  
10 new functionality was submitted in a manner that made an effective check for security problems  
11 infeasible.

12 14. Apple’s August 14 letter to Epic contends (paragraph 3) that the app “[introduced] new  
13 payment functionality that was not submitted to or reviewed by App Review.” Apple’s App Store  
14 Review Guidelines admonish developers to “make sure you...[i]nclude detailed explanations of non-  
15 obvious features and in-app purchases in the App Review notes, including supporting documentation  
16 where appropriate.” (See Schiller TRO declaration, Exhibit C, page 4.) Did Epic provide such  
17 explanation? To find out, I asked Apple for the explanatory text supplied with the pivotal v13.40  
18 version of *Fortnite* (the one that contained the hotfix described by Mr. Grant) at the time it was  
19 submitted to the App Store on August 3, 2020. I show in figure 1, below, a screen capture of that text  
20 with which Apple supplied me. And please note that Apple represents to me that there was no other  
21 material submitted by Epic on August 3 that might have indicated that the update would introduce an  
22 Epic direct payment system, and further represents that there are no other records of Epic having sent  
23 Apple any additional data through Apple support channels.

24 15. The text supplied by Apple as Epic’s submittal description makes no mention of the  
25 new payment option feature. Here is what Epic describes as “What’s New,” in its entirety: “Splash  
26 down into Chapter 2 – Season 3! Survive more than just the Storm in the aftermath of its revenge. As  
27 the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.  
28 Haven’t tried *Fortnite* before? Explore the Island and check out what’s new. Dive in!”

**What's New**

Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.

Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!

*Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.*

*Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!*

*Figure 1. What's New text for Fortnite v13.40 (8/3/20)*

16. Not only does the v13.40 text omit any mention of the significant new non-IAP payment feature, it repeats word for word the *What's New* text for the previous version, v13.30, submitted over two weeks earlier (on July 17) – and matches as well the entirety of the *What's New* text for v13.40.1 (August 6, 2020), submitted three days later. I show these two preceding/following descriptions – almost identical to figure 1 – as figure 2 and figure 3.

**What's New**

Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.

Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!

*Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.*

*Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!*

*Figure 2. What's New text for Fortnite v13.30 (7/17/20)*

**What's New**

Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.

Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!

*Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.*

*Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!*

*Figure 3. What's New text for Fortnite v13.40.1 (8/6/20)*

17. The pattern of repeated *What's New* texts was broken with the next release, v14.00, which was submitted on August 25, 2020, after Apple had removed Fortnite from the App Store. It

says (figure 4), “Update: - Chapter 2 – Season 4 is here, adding a new Battle Pass and new outfits - Continues to offer customers the choice of in-app purchases using either Apple’s payment solution or Epic direct payment.” Nowhere in the text describing “What’s New” in three updates of Fortnite – on August 3, August 6, or August 25 – was the *introduction* of a new feature announced.

#### What's New

##### Update:

- Chapter 2 - Season 4 is here, adding a new Battle Pass and new outfits  
- Continues to offer customers the choice of in-app purchases using either Apple's payment solution or Epic direct payment

*Splash down into Chapter 2 - Season 3! Survive more than just the Storm in the aftermath of its revenge. As the Island adapts to its flooded way of life, stay afloat, take on new enemies and new challenges.*

*Haven't tried Fortnite before? Explore the Island and check out what's new. Dive in!*

*Figure 4. What’s New text for Fortnite v14.00 (8/25/20)*

18. As I mentioned in paragraph 6, Apple tells me that they have terminated 54,805 accounts in the past twelve months for “Hidden features / Code Obfuscation / Facilitating downloading/installing of executable code, etc.” Since the v13.40 *What’s New* text makes no mention of the new payment option, it seems reasonable to me to classify the latter as a hidden feature. And as Epic concedes (Grant Declaration, paragraph 12; Sweeney Declaration, paragraph 9) the effect of the new feature was to “introduce the option for *Fortnite* players on iOS to make in-app purchases using Epic’s own payment system” (op. cit., paragraph 9), it also seems reasonable to me to classify *Fortnite* v13.40 as “introducing a non-IAP payment method,” an outcome for which (see paragraph 6 in this declaration) Apple terminated 1,197 accounts in the past year. For these reasons, Apple’s termination of at least some accounts relating to the v13.40 update seems consistent to me with other actions in the past year.

19. I will turn now to comments on Mr. Philip Schiller’s declaration in support of Apple in opposition to the TRO.

20. Mr. Schiller asserts (Schiller TRO declaration, paragraph 19) that “iOS and the App Store are widely recognized as providing the most secure consumer technology available.... Developers benefit directly and significantly from the security safeguards in this marketplace.” I consider that these good outcomes derive directly from Apple’s App Store review policies and procedures.



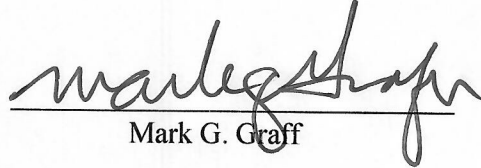
21. Mr. Schiller states (paragraph 18) that Apple “designed the App Store to provide a safe, secure, reliable, and trusted place.... Central to these objectives is Apple’s requirement that every app designed for iOS undergo rigorous, human-assisted review.” I agree with the requirement (and laud the goals). My experience as a programmer, development manager, application security analyst and as a CISO has taught me that well-informed, human-assisted review is fundamental to application security. Obfuscation of (or a neglect to mention) the functionality intended by a software change can significantly complicate the work of any assessor in evaluating the potential security impact of such a change. The interaction of software components when code is executed can be astonishingly intricate, and a sound description of changes and their intent can be essential in devising a road map for effective review or testing. Apple’s approach, curated review, is consistent with best industry practice.

22. Further to that point, if every developer (or even a great many developers) were permitted to implement changes to their applications in the two-stage manner implemented by Epic in this matter, without being required to expressly call attention to the new functionality, I would expect a dramatic impact on App Store security reviews. The extraordinary volume of app submissions, combined with the innate difficulty of finding security issues by mere examination of the software, would make iOS applications significantly less safe – to the detriment of Apple customers, the developers, and all those of us who live in a world with a billion or so active iPhones.

23. I offer three opinions in conclusion. First, Apple’s published App Store review policies and procedures appear to me to be well considered, implementing principles that are necessary to guard against substantial security breaches. The statistics I have cited here suggest to me that Apple has been consistent in proscribing obfuscation and hidden features, two characteristics that hinder effective security review and that I find to be present in Epic’s August 3 submission. Second, when Epic did not disclose the new non-IAP payment feature when submitting its v13.40 Fortnite update to the App Store on August 3, 2020, their omission and the two-stage “hotfix” approach combined, in my opinion, to both obscure the new functionality and obstruct substantive informed review. Third, even if Epic’s hotfix were determined to implement a legitimate contractually conforming feature, the way they performed the update, if allowed to persist and become the norm for other developers, would quickly and ineluctably degrade the effectiveness of Apple’s security reviews, tending to diminish Apple’s

1 ability to prevent app-based attacks and compromises and likely resulting in real increased risks for  
2 Apple's customers, and others, worldwide.

3 I declare under penalty of perjury under the laws of the United States and the State of California  
4 that the foregoing is true and correct, and that I executed this Declaration on September 14, 2020 in  
5 Fayetteville, Arkansas.

6   
7 Mark G. Graff

## **EXHIBIT A**

# MARK G. GRAFF

mark@telligraff.com • [www.markgraff.com](http://www.markgraff.com) • @istopbadguys

## CHIEF INFORMATION SECURITY OFFICER & CONSULTANT

Senior executive with more than 40 years of success within IT, cyber security, national security, and broadcasting. Strategic problem solver with the ability to remain calm in critical situations. Broad range of specialty fields including information security, risk assessment and management, election security, emerging technology, communications, team building and development, security awareness and training, software development, and human cognition. Author of several books and host of radio show/podcast, "CyberMatters with Mark Graff."

### CRITICAL LEADERSHIP INITIATIVES

- Shared cyber security responsibility for protecting America's nuclear secrets over a nine-year period, successfully upholding all security measures and combating attempted breaches.
- Worked with state governments (2018-2019) to identify and address election security risks.
- Expert witness for the Federal Trade Commission in support of product-related litigation (2017-2019).
- Protected largest stock market company in the world from cyberattack.
- Founded cybersecurity collaboration group for World Federation of Exchanges.
- Developed and hosted the first-ever gathering of world stock market security experts, the Defense of International Markets & Exchanges Symposium, in April 2014.
- Established first-ever radio show focusing on bringing cyber security to the general public.
- Expert witness for State of California on electronic voting system software (2008-2009) and U.S. Congress (2000, 2012).
- Co-founder of Para-Protect Services, a startup company that was first to make a profit from managed security services.

### CAREER TRACK

#### CEO & Founder, TELLAGRAFF LLC 2015 to Present

- Established cyber security consulting firm to deliver critical threat and risk evaluation and remediation, C-level and Board-level training and decision support, expert witness services, keynote addresses and presentations to technical and non-technical audiences, and technical product development guidance.
- Established strategic professional relationships/board positions with leading/emerging cyber security firms.
- Cyber expert for national news outlets and publications including CNN International, CBS News, Wall Street Journal.

#### Chief Information Security Officer, NASDAQ QMX 2012 to 2015

- Managed a \$17-20 million budget and led a team of 30 staff to secure worldwide operations and data against cyber-attacks by foreign countries, criminal organizations, and other hostile entities.
- Directed global security policy, awareness and training, quality in software development, risk assessments, and application security.
- Created and hosted the first-ever gathering of Information Security Experts from global exchanges and stock markets, the Defense of International Markets & Exchanges Symposium (April 2014).

#### Chief Cyber Security Strategist, LAWRENCE LIVERMORE NATIONAL LAB 2008 to 2012

- Designed and wrote complex software utility for DOE sites to detect Personally Identifiable Information and other sensitive data on workstations and servers.
- Conducted numerous cyber security research projects and risk analyses, including classified systems.
- Key advisor to senior executive team on cyber policy, strategy, R&D topics, and potential investments.

#### Chief Cyber Security Officer, LAWRENCE LIVERMORE NATIONAL LAB 2003 to 2008

- Led comprehensive Cyber Security Program across unclassified and classified operations, overseeing a \$23 million budget and 60 employees, including teams for incident response, security training and awareness, and internal audits.
- Oversaw regulatory compliance with DOE and NNSA standards, while managing the policy and procedure formulation for internal projects.
- Negotiated compliance schedules and contractual agreements with federal regulatory officials and agencies.
- Spearheaded laboratory-wide FISMA-mandated certification and accreditation program, implementing a Safe Harbor approach to move lab forward while meeting rigid compliance requirements.

**Vice President & Chief Scientist, PARA-PROTECT**

2000 to 2002

- Managed technology forecasting, security trend and threat analysis, and led promotional activities to raise awareness of necessity of secure future for global information infrastructure.
- Assisted in the development and execution of managed security service portfolio, including incident prevention and response.

**Manager, Information Security Deployment, SUN MICROSYSTEMS**

1992 to 2000

- Held a range of increasingly responsible positions from Security Coordinator (1993-1997) to Network Security Architect (1997-1999) to Manager, Information Security Deployment (1999-2000)
- Responsible for corporate global programs to measure security risks and deploy countermeasures, including program and resource development, security awareness training, and lecturing.
- Testified before U.S. Congress, delivered invited lectures to nuclear research laboratories and the American Academy for the Advancement of Science on information security measurement and risk assessment techniques.

**EDUCATION**

UNIVERSITY OF SOUTHERN MISSISSIPPI  
**BS, COMPUTER SCIENCE, 1978**

**CERTIFICATION & TRAINING**

CISSP CERTIFICATION (2017, 2009)  
 FCC AMATEUR EXTRA BROADCAST LICENSE (2009)  
 1000+ HOURS OF COMMERCIAL TRAINING  
 3000+ HOURS OF TECHNICAL TRAINING

**MILITARY EXPERIENCE**

U.S. AIR FORCE  
**COMPUTER TECHNICIAN, 1975-1979**

**BOARDS & ADVISORY ROLES**

DIGITAL AUTHENTICATION TECHNOLOGIES

**BOARD MEMBER**

NETWORK TIME FOUNDATION

**BOARD MEMBER**

BLACKRIDGE TECHNOLOGY

**TECHNICAL ADVISORY BOARD MEMBER**

SECURITY SCORECARD

**TECHNICAL ADVISORY BOARD MEMBER**

FORUM OF INCIDENT RESPONSE & SECURITY TEAMS  
 (FIRST)

**FORMER CHAIR**

LA HONDA-PESCADERO UNIFIED SCHOOL DISTRICT  
**FORMER PRESIDENT & BOARD MEMBER**

**HONORS & AWARDS**

INFORMATION SECURITY EXECUTIVE OF THE YEAR FOR NORTHEAST US, 2014

“KEEP IT SAFE” EDUCATIONAL VIDEO -TELLY AWARD, 2000

TESTIFIED BEFORE CONGRESS 2000, 2012

**SELECTED PUBLICATIONS**

*OFFICIAL (ISC)2 GUIDE TO THE CISSP CBK*  
**Co-AUTHOR, 2019**

*ENTERPRISE SOFTWARE SECURITY*, ADDISON-WESLEY  
**Co-AUTHOR, 2014**

*E-VOTING AND FORENSICS: PRYING OPEN THE BLACK*  
*BOX*

**Co-AUTHOR, 2009***SECURE CODING*, O'REILLY ASSOCIATES**Co-AUTHOR, 2003**

*TWENTY YEARS OF INTERNET SECURITY*, NEXT TWENTY  
 YEARS NEWSLETTER

**AUTHOR, 2001**

*PEXLIB: A REFERENCE MANUAL*, PRENTICE-HALL  
**AUTHOR, 1994**

*HOW NOT TO GO BROKE AS A CONSULTING ENGINEER*,  
 MIDNIGHT ENGINEERING VOL 1, No. 4

**AUTHOR**

*THE ACCESS CONTROL EXECUTIVE: PSYCHOLOGICAL*  
*ELEMENTS OF COMPUTER SECURITY*, MONOGRAPH

**AUTHOR, 1987****SELECTED FEATURES AND OPINION PIECES**

INC., FORBES, USA TODAY, SF CHRONICLE, CSO  
 MAGAZINE, PC MAGAZINE, CNN INTERNATIONAL, CBS  
 RADIO, THE INTERCEPT

**SELECTED SPEAKING ENGAGEMENTS**

“CYBER MATTERS WITH MARK GRAFF”

**RADIO SHOW HOST**

NYIT CYBER SECURITY CONFERENCE (2016)

**KEYNOTE SPEAKER**

ACM CPR SIG (2015)

**KEYNOTE SPEAKER**

SPLUNK CYBER SECURITY CONFERENCE (2014)

**KEYNOTE SPEAKER**

YOUTUBE / TELEGRAFF WEBSITE

**SIXTY-SECOND VIDEO ESSAYS**